UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

Joint Stock Company "Channel One Russia Worldwide," Closed Joint Stock Company "CTC Network," Closed Joint Stock Company "TV DARIAL," Closed Joint Stock Company "New Channel," Limited Liability Company "Rain TV-Channel," and Limited Liability Company "Global Entertainment TV,"

Index No. 16-cv-1318 (GBD)(BCM)

Plaintiffs,

-against-

INFOMIR LLC (www.infomirusa.com), INFOMIR GMBH, ALEXANDER MARAHOVSKY, EVGENI LEVITIN, TELETRANSFERS TECHNOLOGIES LTD., PANORAMA ALLIANCE, LP (www.mypanorama.tv), ASAF YEVDAYEV, DAVID ZELTSER, S.K. MANAGEMENT OF NEW YORK, INC. (www.gudzon.tv), MOIDOM LLC, TELEPROM, VDALI, MHCOM GmbH and John Does 1-50.

Defendants.

----------X

MEMORANDUM IN SUPPORT OF PLAINTIFF BROADCASTERS' JOINT MOTION TO EXCLUDE INFOMIR'S EXPERT TESTIMONY

Table of Contents

I. INTRODUCTION 1

II. PRELIMINARY STATEMENT 2

III. BACKGROUND FACTS 4

A. SUMMARY OF METHODS AND CONCLUSIONS IN ROSENBLATT REPORT AND ROSENBLATT'S DEPOSITION TESTIMONY 4
B. SUMMARY OF METHODS AND CONCLUSIONS IN RUCINSKI REBUTTAL REPORT 7
C. ROSENBLATT AND RUCINSKI DO NOT DOCUMENT THEIR INVESTIGATIONS WITH A PACKET CAPTURE FILE 11

IV. APPLICABLE LAW 11

A. BECAUSE INFOMIR HAS NOT SATISFIED ITS BURDEN OF PROVING BY A PREPONDERANCE OF THE EVIDENCE THAT ROSENBLATT'S TESTIMONY IS ADMISSIBLE UNDER FED. R. EVID 702, IT SHOULD BE EXCLUDED IN ITS ENTIRETY 15
1. Rosenblatt's Testimony Is Not Based on Reliable Methods Because He Did Not Test Infomir's Products Challenged By Broadcasters In The Complaint 16
2. Rosenblatt's Conclusions Regarding Decryption or Hacking are Irrelevant and Inadmissible Because The Complaint Does Not Allege Decryption Or Hacking 17
3. **Rosenblatt's conclusions regarding Infomir Antipiracy measures are irrelevant and inadmissible because he has not investigated DRM system designed by Infomir nor shown that Infomir's DRMs are grounded in industry standard practice 18**
4. Rosenblatt's Testimony Relating To Blacklisting Is Unreliable and Irrelevant 21
5. Rosenblatt's Substantial Non-infringing Use Analysis Is Unreliable and Irrelevant 24
B. BECAUSE INFOMIR HAS NOT SATISFIED ITS BURDEN OF PROVING BY A PREPONDERANCE OF THE EVIDENCE THAT RUCINSKI'S REBUTTAL TESTIMONY IS ADMISSIBLE UNDER FED. R. EVID. 702, IT SHOULD BE EXCLUDED IN ITS ENTIRETY 26
1. Rucinski's Alfabox Test 1 Conclusions That Infomir Has No Control Over STBs Lack A Reliable Methodology 27
2. Rucinski's Bari Alfabox Text 1 Conclusions That Infomir Has No Control Over STBs Lack A Reliable Methodology 28
3. Rucinski's PCAP Analysis Conclusions Relating To Infomir's Lack of Involvement In Unlicensed Streaming Lack A Reliable Methodology 29
4. Rucinski's Analysis of The Effectiveness of Blacklisting Lacks A Reliable Methodology and is Self-Contradicting 31
5. Rucinski's Summaries of Opinions Lack A Reliable Methodology 33
C. (ON BEHALF OF CHANNEL ONE) INFOMIR HAS NOT SATISFIED ITS DAUBERT BURDEN OF SHOWING ADMISSIBILITY BY A PREPONDERANCE OF THE EVIDENCE BECAUSE ROSENBLATT AND RUCINSKI CONSCIOUSLY AVOIDED DISCUSSING AND ANALYZING EVIDENCE OF ILLEGAL STREAMING COLLECTED BY CHANNEL ONE RUSSIA AND BROADCASTERS 33

V. CONCLUSION 39

Table of Authorities

CASES

Amorgianos v Natl. R.R. Passenger Corp., 303 F3d 256, 267 (2d Cir 2002) ----------12, 13, 27
Boucher v. U.S. Suzuki Motor Corp., 73 F.3d 18, 21 (2d Cir. 1996) ----------12
Chill v Calamos Advisors LLC, 417 F Supp 3d 208, 229 (SDNY 2019)----------35
Daubert v Merrell Dow Pharm., Inc., 509 US 579 (1993)---------- 11, 12
DISH Network L.L.C. v. Simmons, No. 4:17-CV-53, 2018 WL 3647169 (E.D. Tenn. June 28, 2018) ----------15
DISH Network LLC v. Cintron, No. 6:12-cv-640, 2013 WL 12385274 (M.D. Fla. Jan. 25, 2013) ----------15
DISH Network LLC v. Lewis, No. 4:19-cv-3125, 2020 WL 1862667 (E.D. Mo. Apr. 14, 2020) 15
DISH Network, LLC v Henderson, 519-CV-1310-MAD-ATB, 2020 WL 2543045 (NDNY May 19, 2020)----------15
Gen. Elec. Co. v Joiner, 522 US 136, 146 (1997) ----------13
Heller v Shaw Indus., Inc., 167 F3d 146, 153 (3d Cir 1999)----------13
In re Mirena Ius Levonorgestrel-Related Products Liab. Litig. (No. II), 341 F Supp 3d 213, 239-240 (SDNY 2018)---------- 12, 13
Joint Stock Co. Channel One Russia Worldwide v Infomir LLC, 16CV1318GBDBCM, 2019 WL 8955234 (SDNY Oct. 25, 2019) ----------14
Kumho Tire Co. v. Carmichael, 526 U.S. 137, 152(1999) ----------14
Nimely v City of New York, 414 F3d 381, 396 (2d Cir 2005)---------- 12, 28
Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012)---------- 22, 33
Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010)---------- 22, 33
Wills v Amerada Hess Corp., 379 F3d 32, 48 (2d Cir 2004)----------12

STATUTES

17 U.S.C. §512(c)(3)(a) ---------- 22, 33
47 U.S.C. §605(a) ---------- 2
47 U.S.C. §605(e)(4)----------2, 14

RULES

Federal Rule of Evidence 401 ---------- passim
Federal Rule of Evidence 403 ---------- passim
Federal Rule of Evidence 702 ---------- passim
Federal Rule of Evidence 703 ---------- passim

I. INTRODUCTION

This Court should exclude Infomir LLC's ("Infomir") expert testimony because it does not meet the requirements for admissibility under the Federal Rule of Evidence 702. The proposed expert testimony is not relevant to the parties' claims that Infomir distributes unauthorized satellite communications or distributes devices with knowledge that such devices are primarily of assistance in distributing unauthorized satellite communications in violation of the Federal Communications Act 47 U.S. §§605(a) and 605(e)(4), or to Infomir's defenses thereto. Nor is the proposed expert testimony the product of reliable principles and methods or based on reliable or admissible evidence as required by Federal Rule of Evidence 703 or otherwise helpful to the trier of fact. Rather than providing truly "expert" opinion testimony, based on reliable scientific principles and methods, Infomir's purported "experts" instead merely offer lay opinions, speculation and hearsay. The core issue in this case is whether Infomir distributes or has knowledge that its set top boxes ("STBs") and software are being used primarily to assist in distributing unauthorized radio or satellite communications. Rather than focus on this issue, Infomir's experts direct most of their efforts on issues that are irrelevant to this case, and reach conclusions that are either unsupported by reliable scientific methodology, or by applying methodologies that are so riddled with fundamental and incurable problems that their testimony is rendered unreliable, irrelevant, and ultimately inadmissible.

The proposed testimony of Infomir's experts William Rosenblatt and Christopher Rucinski should be excluded by this Court in its gatekeeper function under the seminal *Daubert* case and its progeny because it is inadmissible and Infomir cannot, as it is required to do, affirmatively show by a preponderance of the evidence that the proposed testimony is admissible. To demonstrate admissibility under Fed. R. Evid. 702, Infomir is required to show that (i) the expert is qualified, (ii) the testimony is based on sufficient data, (iii) the testimony is the product of reliable methods

reliably applied, and (iv) the testimony is relevant and will assist the jury. Under Fed. R. Evid. 703, expert reports cannot be used as a vehicle for inadmissible hearsay or to put in evidence that has not been fully qualified either by expert authority or that has been vetted as reliable or authentic before the finder of fact. Because Infomir cannot meet its burdens of proof, the expert testimony should be excluded.

II. PRELIMINARY STATEMENT

Because Infomir fails to meet its burden of proof of showing admissibility, the proposed witnesses and their testimony should be excluded. This is an action brought by Plaintiffs (or "Broadcasters") alleging that Defendant Infomir LLC and its affiliates have violated Federal Communications Act of 1934, 47 U.S.C. §605(a) (Unauthorized publication or use of communications) and 47 U.S.C. §605(e)(4) which prohibits distribution of an electronic or mechanical device with knowledge that it will be used primarily to be of assistance in distributing unauthorized satellite communications) by offering a "MAGIC Solution" suite of software (including middleware branded as "Stalker" or "Ministra") and hardware together with MAG 254 and MAG 256 STBs. Infomir markets the MAGIC Solution to businesses as a means of broadcasting television content to consumers in the United States. Broadcasters have alleged that Infomir's customers use the MAGIC Solution to engage in large-scale commercial unauthorized streaming of Russian television content to United States consumers through this "piracy startup kit."

Defendant Infomir has proffered William Rosenblatt ("Rosenblatt") and Christopher Rucinski ("Rucinski") as experts seeking to offer opinions at trial who have submitted reports and been deposed. Neither expert tested Infomir's MAGIC Solution. Neither expert configured the popular Linux-based Infomir MAG 254 or MAG 256 STB with any of the URLs identified by Broadcasters providing pirated versions of Broadcasters' satellite programming to U.S. customers

for monthly subscription fees. Neither expert had information regarding any Infomir notice and takedown procedures. Neither expert examined configured Stalker Middleware in connection with the Infomir MAG STBs. Neither expert provided copies to Broadcasters of the Infomir or other firmware examined in reaching his conclusions and neither expert recorded or retained records of any testing that would enable those tests to be analyzed for accuracy and reliability. Neither expert had knowledge of Infomir's client lists, whether or not those clients were licensed to broadcast, what information Infomir collected from each STB as it is used, or who downloaded Infomir's middleware from Infomir's portal. In addition to relying on inadmissible hearsay, such as conversations with Infomir's deceased President Grigoriy Goldfedib, both experts litter their reports with unreliable, irrelevant speculation and consideration of deliberately misleading questions irrelevant to the subject matter of this action.

Because both experts misstate the issues relevant to the case and merely state opinions based on inadmissible hearsay or unauthenticated statements unsupported by any reliable, repeatable methodology the testimony should be excluded.

Finally, while joining in the remainder of the brief, Plaintiff Joint Stock Company Channel One Russia argues separately below that Rosenblatt's and Rucinski's testimony should be excluded because each has consciously avoided evidence of 3,000 customized Infomir STBs sent to infringer Russian TV Company, has consciously avoided guilty knowledge of Infomir's unauthorized streaming and distribution activities by overlooking passwords provided by Broadcasters to test pirate streams (and indeed recent tests show Infomir still connected to NovoeTV) and thus, due to this "head in the sand" approach related to blacklisting and Infomir's ability to control STBs functions via its Stalker middleware and handshaking, Rosenblatt and Rucinski each have no relevant or reliable testimony related to the claims or defenses confronting

the Court.

III. BACKGROUND FACTS

A. Summary of Methods and Conclusions in Rosenblatt Report and Rosenblatt's Deposition Testimony

Rosenblatt's February 4, 2020 expert report contains 86 numbered paragraphs plus exhibits. ("Rosenblatt Report"). The Rosenblatt Report is attached as Exhibit A to the Declaration of Eugene D. Kublanovsky ("Kublanovsky Decl."). A transcript of Rosenblatt's November 2, 2020 deposition in this case is attached as Exhibit B to the Kublanovsky Decl.

The Rosenblatt Report concludes that Infomir STBs have "substantial non infringing uses" because "Infomir STBs are capable of being used 'out of the box' with non-infringing IPTV services that use DRM []" because "it is not necessary that those DRMs be pre-installed on the STBs when Infomir delivers them to operators or users…." (Rosenblatt ¶ 79). This conclusion is derived almost entirely from three sources: (1) information orally provided to him by Infomir which does not appear to have been independently verified; (2) *ipse dixit*; and (3) incomplete and wholly inadequate observations of products not even at issue in this litigation. The steps Mr. Rosenblatt failed to take and allegations he could have but chose not to evaluate are instructive.

Mr. Rosenblatt begins by recounting the history of the use of STBs in the television business (Rosenblatt ¶¶ 17-33). He notes that a user typically enters a username and password to configure an STB to obtain access to programing. (Rosenblatt ¶ 33). Rather than configure an Infomir STB to receive programming (authorized or unauthorized), he conducted a visual examination of an unconfigured MAG 420w1 STB (*Id.* at ¶ 34). By his own admission, the full extent of Mr. Rosenblatt's own investigation is based on his testing of a total of two (out-of-the box STBs). He does not indicate where he received the STBs and fails to acknowledge that neither of the two STBs he reviewed were the models that are at issue in this litigation and that were

specifically identified by Plaintiffs. Mr. Rosenblatt's report provides no explanation as to why he chose these particular models nor why he did not review the actual models at issue.

He conceded during his deposition that he did not configure an Infomir STB embedded portal with the usernames, passwords, and URLs of unlicensed IPTV providers produced by Plaintiffs and presumably made available to him by Infomir's counsel. (Rosenblatt Tr. 34:20-36:22; 216:16-217:16). In particular, he did not test the Gudzon, NovoeTV or Teleprom passwords. (*Id.* at 89:24-90:9; 107:25-108:1235:2-11).

Mr. Rosenblatt then provides a basic description of an IPTV system and provides a diagram of the system. (Rosenblatt ¶¶ 44-45, Figure 12)(noting "middleware is one component of the architecture that IPTV services build and operate[]" and "middleware runs on a separate server from the sources of content…."). Rather than test a representative configured system, however, Mr. Rosenblatt based his analysis on the review of an Mr. Rosenblatt examined an unconfigured Infomir Stalker 5.3.0 Middleware that is not part of an IPTV system. (*Id.* ¶ 38)(finding it was "only configured with a single 'test channel'…."). He then speculates that Verizon FIOS Middleware that he claimed to have tested has the same functionality as configured Stalker Middleware that he did not test. (*Id.* ¶¶ 40-43). Therefore, Mr. Rosenblatt failed to investigate any IPTV service using Infomir STBs and Stalker Middleware. (*Id.* ¶¶ 44-45). Instead, he relies on a 2018 verbal representation by Mr. Goldfedib that Naicom IPTV uses Stalker Middleware (*Id.* ¶ 42). Rosenblatt later admitted he did not know how many Infomir customers use Stalker Middleware (Rosenblatt Tr. at 159:9-19). Despite not testing any operational IPTV system, he concludes that Infomir STBs do not enable piracy because the STBs themselves do not decrypt content (*Id.* ¶ 83).

Mr. Rosenblatt also opines—*ipse dixit*—that potential antipiracy measures available to Infomir—digital rights management, blacklisting domains, https security and extended validation

certificates—are ineffective. (*Id.* ¶¶ 49-72). He concludes that if any "STB receives unlicensed content that is not encrypted, no DRM will prevent the STB from being able to play it for the user." (*Id*. 63). He bases his conclusion on his opinions of the DRM capabilities of a Google approved MAG 425A Android STB which is different from Linux based MAG STBs, like the MAG 254 and MAG 256 that are not approved by Google. (*Id*. ¶¶ 59-60, 65).

Despite claiming Infomir's antipiracy measures meet industry standards, Mr. Rosenblatt did not compare antipiracy measures of Infomir STBs to other STBs in the market despite claiming "Roku, Apple TV, Samsung Smart TV, or any other STB share the same core functionality of an Infomir." (*Id*. at ¶ 33). In his deposition, Mr. Rosenblatt admitted that certain functionalities of STBs are different. (Rosenblatt Tr. at 180:17-182:9)(stating Roku's programming distribution system through a channel store is an "apples to oranges" comparison with Infomir STBs with only two portals to obtain content). Further, he was uncertain whether Infomir's embedded portal on its MAG STBs was similar to a Roku or Apple TV device. (*Id.* at 174:1-177:25). Rosenblatt also conceded that he did not test an Apple TV to see if it used an embedded portal/browser like Infomir. (*Id*. 177:19-25).

According to Mr. Rosenblatt, Infomir has a different antipiracy procedure than Roku's because Infomir does not operate a channel store like Roku. (*Id.* at 104:21-107:24). He opines that Roku operates a channel store with notice and take-down provisions that is dissimilar from blocking URLs on the embedded portal/browser offered by Infomir that he did not test. (*Id*. 106:17-107:10; 152:25-154:12; 176:15-177:18). Rosenblatt could not recall other Infomir antipiracy programs besides blacklisting. (*Id*. at 99:3-13). He also confirmed that Netflix and Hulu are not available on MAG STBs, which do not offer apps or channels like devices offered by competitors on the market. (*Id.* at 152:25-154:12).

Mr. Rosenblatt based his report on a 2018 verbal representation by Mr. Goldfedib that Infomir has sold STBs to eight legitimate IPTV providers in North and South America. (*Id.* ¶¶ 25-26, 75-76) but did not rely on any sales invoices or contract describing the model of STBs sold, the number of STBs sold to these providers, or any license these providers had with any of the Plaintiff Broadcasters. (*Id.* ¶¶ 25-26, 75-76). During his deposition, Mr. Rosenblatt read notes he took while meeting with Mr. Goldfedib that stated: "These pirate services support Roku, Amazon, Fire, Android TV, et cetera, et cetera, **plus Infomir**. So you'd be saying that these other devices are also pirate devices." (Rosenblatt Tr. at 19:18-22)(emphasis added). Besides MeGoGo and My IndianTV services, Rosenblatt could not identify other consumer uses for an Infomir STB. (*Id*. at 159:13-20).

B. Summary of Methods and Conclusions in Rucinski Rebuttal Report

Rucinski's August 6, 2020 expert rebuttal report consists of 106 numbered paragraphs plus exhibits ("Rucinski Rebuttal") and is offered in rebuttal to the expert report of Plaintiffs' expert, Mr. Jonathan H. Bari. Kublanovsky Decl., Ex. C. Rucinski's October 23, 2020 deposition transcript in this case is found at Kublanovsky Decl., Ex. D.

The Rucinski Rebuttal makes eight conclusions based on his analysis of a (1) The Russian TV Company Inc. MAG 254 Alfabox AKA Rucinski Alfabox, (2) MAG 254 STB AKA Rucinski MAG 254, (3) MAG 256 STB AKA Rucinski MAG 256, (4) The Russian TV Company Inc. MAG 256 Alfabox AKA Bari Alfabox,, (5) MAG 254 STB AKA Bari MAG 254, (6) Infomir STB firmware images, (7) two PCAPs created by Dmitri Dietrich in 2019 of an Alfabox distributing Channel One Programming, and (8) other materials provided by counsel. (Rucinski at 2-3). He testified that he did not examine Stalker Middleware for his report and that he only knows about middleware generally. (Rucinski Tr. at 104:6-13; 113:5-11; 233:16- 24; 234:25-235:4).

First, Mr., Rucinski concluded that the Rucinski Alfabox and the Bari Alfabox do not check a server for firmware updates that is supervised or controlled by Infomir (Rucinski at 10-25). Nevertheless Figure 20 of his report clearly lists "Infomir" as the vendor of the Bari Alfabox. (*Id*. at 24). He also admitted he had not read an Infomir press release that shows Infomir released an identical version of firmware (0.2.18-r7-254) that he identified on the Rucinski Alfabox. (Rucinski Tr. at 100:22-104:5). Nevertheless, he testified he did not know what party or person developed the firmware on the Alfabox nor when that firmware was installed. (*Id.* at 53:7-54:14; 9:9-11:22; 17:13-18;). He did not investigate what IP address the Alfaboxes connected to. (*Id.* at 117:2-8). He did not research what the URL with the name "Stalker Portal" in the Dietrich PCAPs did. (*Id*. at 157:3-159:3). He conceded that he conducted a limited investigation of the Alfabox firmware domain, firmware.IPTVsys.com, and did not know who owns it. (*Id*. at 73:5-80:7). Nor did he conduct an IP address search that would have revealed that Russian TV Company, Inc. affiliate Techstudio and owner Steven Rudik appear as contacts on this IP address domain block. (*Id*. at 82:22-91:17; 94:10-15).

Second, Mr. Rucinski concludes that the Rucinski Alfabox and the Bari Alfabox are not "plug-and-play" STBs because the MAC addresses had been blocked. (Rucinski at 26-31). However, he conceded that he did not call a customer service phone number that appeared on the STBs to activate the STB. (Rucinski Tr. at 114:15-24; 25:7-11).

Third, Mr. Rucinski concludes that Infomir does not "participate[] in" sending unlicensed content to STBs configured with the Alfabox software (Rucinski at 32-36). However, he admitted that he would need to do more research to determine if the Infomir STBs communications with Infomir URLs are a "handshake." (Rucinski Tr. 159:16-23). The focus of Rucinski's analysis was a review of two PCAPs collected by Dmitri Dietrich in 2019 showing unauthorized streaming by

Russian Television Company, Inc. (Rucinski at 32-36). However, Rucinski did not investigate what information was being transmitted to or from the Dietrich Alfabox because he stopped his analysis of the Dietrich PCAP after he determined no video content was transferred from Infomir to the STB. (*Id*. at 139:3-151:4). He then speculated that JSON or JavaScript references found in the Dietrich PCAP may have useful information about what information Infomir sends or receives from an STB, but he did not conduct any further investigation. (*Id*. at 153:8-155:12). He confirmed that he knows that Infomir customizes STBs. (*Id.* at 126:12-15). However, he did not investigate or have knowledge of when --- or how --- the customization of the Alfabox occurred. (*Id*. at 64:20-24).

Fourth, Mr. Rucinski found that a June 13, 2017 Infomir firmware update to the Rucinski MAG 254 and MAG 256, not present on the Bari MAG 254, can provide limited domain blacklisting (Rucinski at 37-97). During his deposition, he acknowledged that Infomir did not produce the firmware images he examined. (*Id*. at 128:2- 137:13). He did not know if Infomir initiated any blacklisting via firmware prior to June 13, 2017. (*Id*. at 169:2-9). He did not test when firmware was installed on the STBs and described the process of finding "high fidelity" information on this issue as difficult and expensive. (*Id*. at 27:25-42:16). He did not review a firmware downgrade affidavit produced by Broadcasters giving instructions on how to access pirates streams on MAG STBs nor did he review forums describing how to circumvent Infomir firmware updates on MAG STBs. (*Id.* at 186:11-188:19). *See also* Dowd Decl. Ex. B (Downgrade Affidavit). Confronted with his prior inconsistent testimony in another litigation, Rucinski disputed that testing all versions of the firmware necessary to understand its function. (*Id*. at 249:13-256:19).

Fifth, Mr. Rucinski opined that blocking Mac addresses is not an effective or practical

solution to restrict or prevent broadcasting of unlicensed IPTV content on Infomir STBs (Rucinski at 98-99). He noted in his report that during his purported "test" the Bari Alfabox tried to "authenticate itself, but the request was rejected" due to its MAC address being blocked (Rucinski at 28- 31; Figures 26, 29). Rucinski also did not "monitor the network communications" to see what server blocked the Rucinski Alfabox Mac address. (Rucinski Tr. 108:15-24). Rather, he speculated that "some server which then attempted to perform some authentication on it and in response to that procedure determined that as stated in figure 26 that your MAC address is not in the system." (*Id*. 109:2-6).

Sixth, Mr. Rucinski speculated without any testing of Infomir STBs that blacklisting domains is an ineffective antipiracy measure (Rucinski at 99-102). He speculates that blacklisting "may do more harm than good" because the domain may distribute a mix of licensed and unlicensed content. (*Id*. at 100). However, he does not know the identities of Infomir's bulk customers or whether or how many Infomir STBs are sold retail directly to U.S. consumers. (Rucinski Tr. at 98:7-99:13; 120:17-21; 121:9-15; 190:6-11). He also did not test the passwords provided by Broadcasters on an Infomir STB. Instead, tried NovoeTV and Teleprom passwords on his computer browser and kept no records of his access to those video streams. (*Id*. at 44:11-20).

Seventh, Mr. Rucinski concluded that preinstalled DRMs on Infomir STBs are irrelevant to whether such devices are designed to use content in an unlicensed manner (Rucinski at 103-04). However, he did not confirm the Rucinski STBs used the Linux operating system. (*Id*. at 192:10-11). Rucinski also disagrees with Bari about the viability of DRMs, but does not test Infomir STBs to see if the embedded portal/ browsers have DRM compatibility. (Compare Rucinski at 2-4 to 103-04).

Eighth, Mr. Rucinski speculated that the use of either HTTP or HTTPS on a server computer configured to distribute IPTV content is irrelevant to whether the server distributes licensed or unlicensed content (*Id*. at 105-06). However, Rucinski's analysis is limited to "the use of either http or https on a server computer rather than STB. *(Id.)*

C. Rosenblatt and Rucinski Do Not Document Their Investigations with a Packet Capture File

A network protocol analyzer or "WireShark… is a software program that allows a user to create a record of data packets transmitted across a computer network by 'capturing' the data packets in a file[]"called a PCAP." (September 26, 2019 Order (ECF 779) at 10 quoting Nov. 3, 2018 Rucinski Report). A "PCAP contains the full data payload that gets sent or received." (2018 Rucinski Report (ECF 694-1) at 9). Rosenblatt conducted no Wireshark tests for his report because, according to him, that PCAP detail was not necessary for what he was doing and he was not competent to testify what a protocol in a Wireshark file signifies. (Rosenblatt Tr. at 61:2-16; 131:17-132:4). Similarly, Rucinski did not create a PCAP or use a network protocol analyzer while conducting any of his investigations. (Rucinski Tr. at 47:8-48:2; 114:25-116:25; 168:8-12).

IV. APPLICABLE LAW

In interpreting Fed. R. Evid 702 the Court must determine whether the evidence is relevant and reliable. "[U]nder the Rules the trial judge must ensure that any and all scientific testimony or evidence admitted is not only relevant, but reliable." *Daubert v Merrell Dow Pharm., Inc.*, 509 U.S. 579, 589 (1993). To meet the requirements of Fed. R. Evid. 702 "the party seeking to admit expert testimony must show by a preponderance of the evidence that: (i) the expert is qualified, (ii) the testimony is based on sufficient data, (iii) the testimony is the product of reliable methods reliably applied, and (iii) [*sic*] the testimony is relevant and will assist the jury." *In re Mirena Ius Levonorgestrel-Related Products Liab. Litig. (No. II),* 341 F. Supp. 3d 213, 239-240 (S.D.N.Y.

2018), *affd sub nom. In re Mirena IUS Levonorgestrel-Related Products Liab. Litig. (No. II)*, 982 F.3d 113 (2d Cir. 2020).

Under *Daubert*, trial courts serve as "gatekeepers," responsible for ensuring that an expert's testimony is based upon a reliable foundation and is relevant to the task at hand. *See Daubert*, 509 U.S. at 597. "In gauging reliability, the district court should consider the indicia of reliability identified in Fed. R. Evid. 702, namely, (1) that the testimony is grounded on sufficient facts or data; (2) that the testimony is the product of reliable principles and methods; and (3) that the witness has applied the principles and methods reliably to the facts of the case." *Wills v Amerada Hess Corp.*, 379 F.3d 32, 48 (2d Cir. 2004). To warrant admissibility, however, it is critical that an expert's analysis be reliable at every step." *Amorgianos v Natl. R.R. Passenger Corp.*, 303 F.3d 256, 267 (2d Cir. 2002).

It is well settled that in order to be admitted, expert testimony must be based on sufficient data and be the product of reliable methods of analysis reliably applied. In order for the data and methods to be reliable, it must meet some industry standard for sufficient rigor; it cannot be mere conjecture. "Expert testimony should be excluded if it is speculative or conjectural" *Boucher v. U.S. Suzuki Motor Corp.*, 73 F.3d 18, 21 (2d Cir. 1996), or where the proffered opinion is "based on data, a methodology, or studies that are simply inadequate to support the conclusions reached." *Amorgianos* 303 F.3d at 266. Furthermore, an expert witness may also be excluded if his or her proposed methodology is not sufficiently rigorous at each step. "[R]eliability within the meaning of Rule 702 requires a sufficiently rigorous analytical connection between that methodology and the expert's conclusions." *Nimely v City of New York*, 414 F.3d 381, 396 (2d Cir. 2005). Expert testimony simply cannot be admitted if there is insufficient data and a huge gap in logic between the data presented and the expert's resulting opinion. "A court may conclude that there is simply

too great an analytical gap between the data and the opinion proffered" *Gen. Elec. Co. v Joiner*, 522 U.S. 136, 146 (1997).

In addition, courts consider the actual analysis employed by the proffered experts in reaching their conclusions and the analysis must clearly lead to the conclusions. "Courts have found analytical gaps to be too great, for example, when a critical step in a prospective expert's reasoning is based on a highly dubious analogy. See, e.g. *Mirena Perforation/Daubert*, 169 F. Supp. 3d at 439 ('Such a subjective comparison of muscle of a pig heart to a female uterus creates simply too great an analytical gap between the data and the opinion proffered to pass muster under Rule 702 and *Daubert*.' (quotation marks omitted)); *Shatkin v. McDonnell Douglas Corp.*, 727 F.2d 202, 208 (2d Cir. 1984) (rejecting expert methodology based on an 'apples and oranges' comparison)." *In re Mirena*, 341 F. Supp. 3d at 241.

Notably, while the appropriate focus of the *Daubert* analysis is on the principles and methodology employed rather than the conclusions drawn, "a district court must examine the expert's conclusions in order to determine whether they could reliably follow from the facts known to the expert and the methodology used." *Heller v Shaw Indus., Inc.*, 167 F.3d 146, 153 (3d Cir. 1999).

In addition to the requirements of Rule 702, expert testimony is also subject to the relevancy requirement under Federal Rule of Evidence 401. *In re Platinum-Beechwood Litig.*, 469 F. Supp. 3d 105, 114 (S.D.N.Y. 2020). Further, under Federal Rule of Evidence 403, "the Court may still exclude relevant evidence 'if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues [or] misleading the jury…." *Id.* quoting Fed. R. Evid. 403. "The Rule 403 [probative value] inquiry is particularly important in the context of expert testimony, 'given the unique weight such evidence may have in a jury's

deliberations.'" *A.V.E.L.A., Inc. v. Estate of Marilyn Monroe, LLC*, 364 F. Supp. 3d 291, 325 (S.D.N.Y. 2019) (citation omitted).

Finally, an expert is expected to "employ[ ] in the courtroom the same level of intellectual rigor that characterizes the practice of an expert in the relevant field." *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 152 (1999). Under Rule 703 of the Federal Rules of Evidence, inadmissible hearsay must be excluded and does not become admissible solely by virtue of its inclusion in an expert report. *Rodriguez v. Modern Handling Equip. of NJ, Inc*., 604 F. Supp. 2d 612, 622 (S.D.N.Y. 2009).

Section 605(a) of the Federal Communications Act "does not include the word 'interception.' Instead, it prohibits 'receiv[ing]" or "assist[ing] in receiving" radio communications by a person "not being entitled thereto ... for his own benefit or for the benefit of another not entitled thereto.'" *Joint Stock Co. Channel One Russia Worldwide v Infomir LLC*, 16CV1318GBDBCM, 2019 WL 8955234, at *11 (S.D.N.Y. Oct. 25, 2019), report and recommendation adopted sub nom. *Joint Stock Co. "Channel One Russia Worldwide" v Infomir LLC*, 16CIV1318GBDBCM, 2020 WL 1467098 (S.D.N.Y. Mar. 26, 2020) (internal punctuation modified). Section 605(e)(4) prohibits the import, sale, or distribution of a "device or equipment" with knowledge that "the device or equipment is primarily of assistance in the unauthorized decryption of satellite cable programming." 47 U.S.C. § 605(e)(4). Section 605(e)(3)(C)(i)(II), in turn, permits a person aggrieved by a violation of § 605(e)(4) to recover statutory damages of $10,000 to $100,000 "for each violation." 47 U.S.C. § 605(e)(3)(C)(i)(II). *Joint Stock Co. Channel One Russia Worldwide v Infomir LLC*, 16CV1318GBDBCM, 2019 WL 8955234, at *6.

Computer software and access codes used to access unauthorized content are "devices" within the meaning of Section 605(e)(4). *DISH Network, LLC v Henderson*, 519-CV-1310-MAD-

ATB, 2020 WL 2543045, at *6 (N.D.N.Y. May 19, 2020) ("The Device Codes, which Defendants sold individually and preloaded onto a set-top box, were designed and produced for purposes of allowing access to the servers that support the Services, and thus are a "device" or "equipment" for purposes of Section 605(e)(4)."") *DISH Network LLC v. Lewis*, No. 4:19-cv-3125, 2020 WL 1862667, *2 (E.D. Mo. Apr. 14, 2020) (holding that the sale of passcodes meant to circumvent security measures enacted by the satellite provider falls squarely within the conduct prohibited by Section 605(e)(4)); *DISH Network L.L.C. v. Simmons*, No. 4:17-CV-53, 2018 WL 3647169, *5 (E.D. Tenn. June 28, 2018) ("Based on the volume of purchased IKS Server Passcodes, Simmons willfully violated the FCA because he knew or should have known that the codes were unlawful"), *report and recommendation adopted*, 2018 WL 3623764 (E.D. Tenn. July 30, 2018); *DISH Network LLC v. Cintron*, No. 6:12-cv-640, 2013 WL 12385274, *2 (M.D. Fla. Jan. 25, 2013) (holding that the defendant violated Section 605(e)(4) through the unauthorized distribution of passcodes that permitted the purchasers to access, receive, intercept, and decrypt DISH Network programming).

VI. ARGUMENT

A. BECAUSE INFOMIR HAS NOT SATISFIED ITS BURDEN OF PROVING BY A PREPONDERANCE OF THE EVIDENCE THAT ROSENBLATT'S TESTIMONY IS ADMISSIBLE UNDER FED. R. EVID 702, IT SHOULD BE EXCLUDED IN ITS ENTIRETY

This Court should exclude Infomir's expert testimony because Infomir has failed to meet its burden of proof of demonstrating that the proposed expert testimony meets the requirements for admissibility under Fed. R. Evid 702. The proposed evidence is not the product of reliable principles and methods and is not helpful to the trier of fact in understanding the evidence or determining the facts at issue. Rather than providing expert opinion testimony, based on reliable scientific principles and methods, which are relevant to the core issues in this case, and which

could be valuable to a trier of fact, Infomir's purported "experts" instead merely offer evasive lay opinions unsupported by any reliable, repeatable methodology required by Fed. R. Evid 702.

The testimony submitted by both of Infomir's experts fails to meet the basic requirements for admissibility under Fed. R. Evid. 702 and 703 and *Daubert* and therefore should be excluded. Here, Infomir's expert testimony is not based on sufficient reliable data or authenticated evidence, the testimony is not the product of reliable methods reliably applied, the testimony is not relevant or reliable and therefore will not assist the jury.

1. Rosenblatt's Testimony Is Not Based on Reliable Methods Because He Did Not Test Infomir's Products Challenged By Broadcasters In The Complaint

The purported "expert testimony regarding technologies and industry practices related to the products and services at issue in the litigation," is --- to the contrary ---- not related to any of the allegations of the complaint and not grounded in any inspection of the Infomir's actual working MAGIC solution product delivered to consumers via IPTV streaming in a combination of hardware (an STB) and software (Stalker/Ministra middleware). Rosenblatt Report ¶ 1 There is no evidence in the record showing that Infomir has sold any unconfigured MAG boxes directly to any U.S. consumers. Mr. Rosenblatt (1) ignores the Complaint's allegations relating to Infomir's complete business-to-business ecosystem of technologies—firmware and middleware— that enable Infomir STBs to facilitate piracy, namely the MAGic solution, (2) misleadingly conflates all MAG STBs because the reports analyze the Google approved MAG 425A Android STB which is unrepresentative of the vast majority of the Linux-based STBs Infomir has sold in the United States, including the MAG 254 and MAG 256 Alfabox, (3) fails to analyze Infomir's popular Stalker a/k/a Ministra Middleware in a working configuration, (4) speculates about potential digital rights management ("DRM") systems that may be downloaded onto an unrepresentative MAG

425A Android STB to conclude that "Infomir's STBs are capable of being used 'out of the box' with non-infringing IPTV services that use DRM." Rosenblatt ¶ 79, and (5) adopts unreliable methods of analysis to reach his conclusions. Because Rosenblatt offers opinions about the wrong Infomir products and unconfigured STBs and is not based on any actual testing of a working product, his testimony is irrelevant and misleading and should be excluded. *See* Fed. R. Evid. 401, 702. Similarly, his conclusions relating to substantial non-infringing uses of Infomir's products are equally inadmissible because they are speculative and not the product of any reliable methods or grounded in any admissible or reliable evidence.

2. Rosenblatt's Conclusions Regarding Decryption or Hacking are Irrelevant and Inadmissible Because The Complaint Does Not Allege Decryption Or Hacking

The conclusions of the Rosenblatt Report regarding STB "decryption" or "hacking" should be excluded as irrelevant to this case because the Complaint does not allege such activities. *See* Fed. R. Evid. 401, 702. Mr. Rosenblatt addresses whether "Infomir STBs have been designed, modified, or hacked to enable decryption of video content that has been encrypted using any of the generally accepted DRMs." Rosenblatt ¶¶ 64-65. However, a STB's ability to hack or decrypt is simply not a relevant issue in this case because this was not alleged in the Complaint. The relevant allegations are that Infomir STBs are sold to broadcasters who have no broadcasting licenses and intentionally designed to connect to Infomir's billing middleware so that a user can connect them to unauthorized pay TV operators, without any verification, screening, or compliance controls and that the unauthorized operator can control access to the STBs by selling codes that the software uses to authorize the video streams. The key differentiator between Infomir's products, and those of its admitted competitors (e.g., Apple and Roku), is that Apple and Roku are not designed to enable their users to connect their STBs to unlicensed, pirate TV networks, nor are

they marketed to known pirates. Rosenblatt at 12 (identifying Apple and Roku as competitors of Infomir).

3. Rosenblatt's conclusions regarding Infomir Antipiracy measures are irrelevant and inadmissible because he has not investigated DRM system designed by Infomir nor shown that Infomir's DRMs are grounded in industry standard practice

Mr. Rosenblatt' conclusions about the efficacy and availability of Infomir's antipiracy measures (if any) should be excluded because they are not grounded in industry practice and are therefore unreliable. *See* Fed. R. Evid. 401,702. Rosenblatt generalizes that "DRM technologies are used in video content services that are licensed by major Hollywood studios and TV networks." Rosenblatt ¶¶ 52. He notes that DRM/conditional access systems are part of an IPTV platform. Id. ¶ 45. However, Rosenblatt conducts no investigation of any Infomir platform that implements DRM/CAS. Rather, he cites to testimony of Mr. Goldfedib about conversations Mr. Goldfedib purportedly had with Rodeo Networks about Fox programming DRM requirements. *Id*. ¶ 53.

The Complaint's allegations and the evidence in this case makes clear that Infomir has no system in place checking to ensure that the Stalker a/k/a Ministra middleware and/or operator is authorized to stream the content, and, in turn, stopping any unauthorized streaming of protected content by the middleware/operator. Rosenblatt admits that Infomir's embedded portal feature allows users to simply enter a URL and credentials to view programming and that the embedded portal terminology is "unique" to Infomir devices. Rosenblatt Tr. 175:6-15-177:4. Rosenblatt's report does not identify DRM capabilities on the MAG 254. Instead, he speculates that all Infomir STBs are capable of the same DRMs as the Google approved MAG 425A Rosenblatt ¶ 59.

However, Rosenblatt (andRucsinski) does not describe how the portal architecture of the Infomir STB interacts with Stalker Middleware, as Rosenblatt admits occurs in his rebuttal.

(Rosenblatt Rebuttal ¶ 30). Rosenblatt also concedes that that Infomir STBs functionality, with a mere two portals, is fundamentally different from the Roku channel store. Rosenblatt Tr. 180:17-182:9. Neither does Rosenblatt explains how the embedded portal can support DRMs. Dietrich identified evidence that the embedded portal, a simple browser, cannot support DRMs. (Dietrich Rebuttal ¶¶139-52). Rosenblatt and Rucinski's conclusions about DRM capabilities on Infomir STBs are not only unreliable, but misleading and evasive.

Infomir could easily avoid piracy by, for example, requiring operators that want to operate legitimate TV networks to register with Infomir. Or, alternately, Infomir could participate in the DMCA notice-and-takedown procedures generally prescribed by U.S. copyright law, allowing content owners that discover piracy occurring on Infomir boxes to report it and have such content blocked. Mr. Rosenblatt later speculated that blacklisting domains could be considered a form of notice and takedown. (Rosenblatt Tr. at 98:17-99). However, he could not recall other Infomir antipiracy programs besides the blacklisting requested by Plaintiffs in this case. (*Id*. at 99:3-13).

Even such minimal efforts or design changes by Infomir would prevent illicit pirate businesses from using Infomir's STBs and "Stalker" or "Ministra" middleware and MAGic solution service as ready-made piracy startup kits. Importantly, this is why the other STBs which Infomir considers competitor products (e.g., Roku and Apple TV) are not used for piracy. Rosenblatt at 12 (identifying Apple and Roku as competitors of Infomir). STBs produced by legitimate vendors such as Roku, Apple TV, Samsung cannot simply be pointed at an unlicensed "operator" and used to play pirate content. This is because those STB makers (e.g., Apple, Roku, etc.) proactively restrict the servers and or middleware with which their boxes can connect in order to prevent piracy. *See e.g.*, fn 1-2 below (describing Roku antipiracy measures).

Mr. Rosenblatt's testimony with respect to anti-piracy software such as Irdeto is similarly

irrelevant, unreliable and misleading. *See* Fed. R. Evid. 401, 403 Rosenblatt argues that the Irdeto Whitepaper "does not specify industry standards" and that Irdeto is aimed at "content providers" (e.g., pay TV operators) rather than STB makers – and that it is not relevant to STB makers because it deals with operators choosing STBs rather than designing them. Rosenblatt at ¶¶71-72. However, the relevance of the Irdeto Whitepaper is not that it discloses about any specific industry standard – rather it is that the use of anti-piracy platforms is an industry standard. In other words, Irdeto and similar anti-piracy platforms are used by legitimate businesses—both STB makers and operators—to prevent piracy. *See* Fed. R. Evid. 401,702. Were Infomir to forbid connections between its STBs and operators that don't implement anti-piracy software like Irdeto, Infomir's STBs would be worthless to pirate operators. By contrast, Infomir's open platform makes the STBs desirable to pirates.

Contrary to Rosenblatt's analysis, the relevant issue here is not whether any particular software or computer protocol is an industry standard that Infomir is not in compliance with. Rather, the issue is that the industry standard - among legitimate STB manufacturers and pay TV operators - is to use anti-piracy software to reduce piracy, theft of satellite signals, and copyright infringement. By deciding to implement anti-piracy measures, Infomir's competitors, Apple and Roku, have pre-vetted their business partners to ensure that such broadcasters are copyright-compliant (legitimate TV networks such as CBS and HBO) and customers (those networks' subscribers.). By deciding not to implement such anti-piracy measures, Infomir likewise has chosen as its business partners, namely pirate TV networks such as Teleprom NovoeTV, and Russian TV Company, and as its customers, namely consumers seeking to steal pay TV services, including those owned by Plaintiff Broadcasters.

For the foregoing reasons, Rosenblatt's analysis and conclusions with respect to

decryption, hacking, industry standards, and the Irdeto Whitepaper are misleading and irrelevant, would not help a jury or trier of fact but, instead, would mislead. *See* Fed. R. Evid. 401, 403, 702 Accordingly, the proposed testimony found at ¶¶ 64-66 and 68-72 of the Rosenblatt Report should be excluded.

4. Rosenblatt's Testimony Relating To Blacklisting Is Unreliable and Irrelevant

Rosenblatt also offers *ipse dixit* opinions, unmoored in industry literature, on the meaning and efficacy of the concept of blacklisting to a degree that renders his testimony unreliable, misleading, and unhelpful to a fact-finder. *See* Fed. R. Evid.401, 403.

Rosenblatt considers "https security, blacklisting and extended validation certificates" and concludes (without support) that "none of these technologies . . . are generally accepted as effective for anti-piracy purposes." Rosenblatt ¶66. Rosenblatt's testimony related to blacklisting and security measures is misleading because the issue is not whether any individual technology is, on its own, a sufficient or generally accepted anti-piracy technology. Rather, those technologies are building blocks that are generally used to implement anti-piracy policies and systems. Infomir's failure to implement blacklisting and security measures is an indication that Infomir does not want to control piracy; rather it wants to be in the business of enabling piracy by providing middleware to pirate TV operators, offering the MAGic Solution service, and selling STBs to content stealing consumers and operators.

Blacklisting is generally understood to be "a basic access control mechanism that allows all elements (…users, URLs, IP Addresses, domain names, …) except those explicitly mentioned. Those items on the list are denied access." In the context of piracy prevention, a simple blacklisting scheme for STBs might involve (i) an STB manufacturer publishing a "blacklist" of known pirate TV operators on its website, (ii) that manufacturer designing its STBs to refuse to

connect to the pirate operators on the list, and (iii) the manufacturer updating the list from time to time as new pirate TV operators are reported or identified, for example in response to copyright owner DMCA complaints.

Moreover, Rosenblatt's analysis ignores a practical and effective way to blacklist infringing content on a massive scale which is recognized by the courts and baked into the Copyright Act – the DMCA Notice and Takedown Procedure. *See* 17 U.S.C. §512(c)(3)(a). "Infomir considers Apple and Roku STBs to be competitors of its STBs." Rosenblatt at ¶33 (citing Goldfedib Dep., 206:23-25). Pursuant to the DMCA Notice and Takedown Procedure, both Apple and Roku provide forms where content owners can simply and easily request that copyright infringing content be removed from their services. Indeed, the *Viacom v. Youtube* line of cases, decided in this District, show that "the DMCA notification regime works efficiently: when Viacom over a period of months accumulated some 100,000 videos and then sent one mass take-down notice on February 2, 2007, by the next business day YouTube had removed virtually all of them." *Viacom Int'l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 524 (S.D.N.Y. 2010), *judgment overturned on other grounds by Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012).

Worse, Rosenblatt's testimony that blacklisting is not an effective anti-piracy measure is refuted by the testimony of Infomir's other expert Rucinski, whose testimony illustrates that Infomir's blacklisting acted as a barrier to his use of the STB to access a pirate website. Rucinski Rebuttal at 37-38. Specifically, when the Infomir boxes tested by Rucinski were updated with Infomir firmware that supported blacklisting, Rucinski reported that he was unable to access known commercial pirate IPTV streaming operations such as NovoeTV. Rucinski Rebuttal at 71. Infomir cannot have it both ways. Because the contradiction between Infomir's two experts on this issue cannot be reconciled, Rosenblatt's testimony on blacklisting and security measures should

be excluded.

The other technologies disparaged by Rosenblatt (HTTPS and/or Extended Validation certificates) are useful because they are the building blocks of effective anti-piracy measures, including but not limited to blacklisting. He argues that "[t]he ability for an STB to support HTTPS is irrelevant to any determination of whether the STB is capable of receiving unlicensed IPTV content." Rosenblatt ¶ 68. However, he offers no factual or logical support for this statement. For example, he could have, but did not, compare antipiracy measures implemented by legitimate pay TV operators (e.g. HBO, Disney Channel, Netflix) or STB manufacturers (e.g. Roku, Samsung) and discussed whether they use HTTPS, extended validation certificates, and/or DRM. (*N.B.* they do!)

Mr. Rosenblatt's failure to reliably compare Infomir's embedded portal architecture to Roku is a fundamental mistake in defending Infomir's DRM capabilities and anti-piracy strategies with a device maker Infomir identifies as a competitor. Roku's channel approval system creates a "walled garden" of potential users of its device [1] Roku thus has a proactive antipiracy system that evaluates licenses prior to being able to distribute programming on a Roku. By contrast, Infomir knows or should know that its STBs have a vulnerable technology, the embedded portal, incapable of DRM protection or proactive monitoring. (Rosenblatt at 152:25-154:12). Roku also advertises that DRMs are built into its devices.[2] This contradicts Rosenblatt conclusion that "It is not necessary that those DRMs be pre-installed on the STBs when Infomir delivers them to operators or users **…** for them to be usable on non-infringing IPTV services." (Rosenblatt ¶ 79).

[1] https://developer.roku.com/docs/features/how-channels-work.md (describing "the three main requirements for creating a Roku channel [as]: [1]Original and/or licensed video content.[2] A place to host your content on the web (for example, an OVP, CDN, and so on).and [3] A feed, which brings your content onto the Roku platform.").
[2] https://developer.roku.com/docs/features/security.md ("Roku takes copyright protection seriously. Built into every Roku device is some of the broadest support of Digital Rights Management (DRM) formats. From streaming protocols to authenticated SSL connections, publishers can bring their content to the Roku Platform with the proper security standards in place.").

Rosenblatt's failure to provide industry data renders his conclusions fatally unreliable and inadmissible. *See* Fed. R. Evid. 401, 403, 702. Similarly, Rosenblatt failed to support his arguments with any evidence that Infomir's competitors provide STBs that mandate HTTPS, extended validation certificates, and DRM; but that such measures failed to curb copyright infringement or pirate operators. Again, his failure to provide industry data to support his arguments renders his conclusions scientifically unreliable—and patently unbelievable. In sum, Rosenblatt simply offered no underlying reliable methodology or rational scientific basis for his remarks as to various anti-piracy technologies and utterly lacks the requisite "sufficiently rigorous analytical connection between that methodology and the expert's conclusions." *Nimely v City of New York*, 414 F.3d at 396.

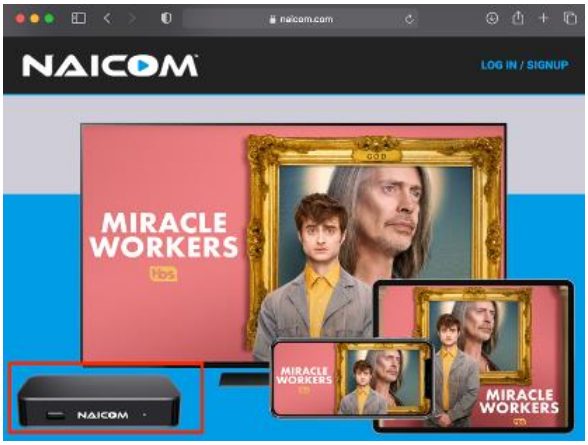
Because Infomir has failed to meet its burden of proof of showing by a preponderance of the evidence that Rosenblatt's proffered testimony with respect to antipiracy measures such as blacklisting, HTTPS, extended validation certificates, and DRM is complete, reliable, and the product of a reliable scientific methodology, it should be excluded.

5. Rosenblatt's Substantial Non-infringing Use Analysis Is Unreliable and Irrelevant

Rosenblatt's analysis and conclusions regarding whether there are "substantial non-infringing uses" for the accused STBs must be excluded because it is unsupported by admissible or reliable evidence and is misleading, irrelevant, and not the product of a reliable scientific methodology.

Rosenblatt testifies that "Infomir's STB products as well as Ministra middleware are currently engaged in uses that I understand to be non-infringing," (referring to Rosenblatt ¶¶ 25-26). ¶74-75. However, paragraphs 25 and 26 of the Rosenblatt Report do not refer to Infomir's unbranded, user and operator configurable STBs such as the MAG 256, which are actually at issue

in this litigation. Rather, those paragraphs refer to Infomir's white-label products which have never been produced in discovery are and that are branded and configured to work only with a particular provider, e.g. Naicom in Puerto Rico. Rosenblatt ¶25.



A screenshot of Naicom's website taken on 10 Feb. 2021.
(from https://naicom.com/index.html)

Importantly, while Rosenblatt identifies various operators that (according to him, though unsupported by any evidentiary record) use Infomir STBs in a non-infringing fashion, he does not testify or even address whether the STBs sold to those operators are the same "unlocked" STBs which are user configurable to connect to pirate TV networks like the MAG 254 or MAG 256. While there may be some Infomir products which are used by legitimate TV operators (e.g. Naicom), this "apples to oranges" comparison should be rejected because Infomir has failed to establish and Rosenblatt has offered no testimony establishing that those products are the same products at issue in this litigation.

The Rosenblatt Report reflects no personal knowledge of any of the uses of Infomir's MAGIC solution product. In other words, while his testimony is addressed to purported "Substantial Non-infringing Uses" of Infomir's products, he fails to present any relevant evidence or opinions on whether the accused products have non-infringing uses, because his testimony relates to Infomir products generally rather than the specific unlocked MAG 254 and MAG 256

products accused of facilitating infringement and piracy in this case. *See* Fed. R. Evid. 401, 403. Further, because Rosenblatt's testimony draws no distinction between different Infomir products (e.g. MAG 256 STBs or Alfaboxes vs. Naicom branded products), his report fails to provide sufficient information to establish, according to any reliable scientific method, that any non-infringing uses are substantial rather than incidental or insubstantial. Thus, his conclusions do not "reliably follow from the facts known to the expert and the methodology used." *Heller v Shaw Indus., Inc.*, 167 F.3d at 153

Thus, for the reasons discussed above, Rosenblatt's testimony regarding purported "non-infringing uses" of the accused products is inadmissible because it is misleading, and because Rosenblatt has failed to establish that it is based on sufficient data or reliable scientific methodologies reliably applied. Because Infomir has failed in its burden of showing that Rosenblatt's testimony found at ¶¶74-79 is admissible under Fed. R. Evid 702, it should be excluded.

B. BECAUSE INFOMIR HAS NOT SATISFIED ITS BURDEN OF PROVING BY A PREPONDERANCE OF THE EVIDENCE THAT RUCINSKI'S REBUTTAL TESTIMONY IS ADMISSIBLE UNDER FED. R. EVID. 702, IT SHOULD BE EXCLUDED IN ITS ENTIRETY

Rucinski's testimony should be excluded because Infomir cannot meet its burden of proof by establishing by a preponderance of the evidence that Rucinski's testimony is relevant or reliable within the meaning of Fed. R. Evid 702 as elaborated in the *Daubert* case and its progeny. The Rucinski Rebuttal is not the product of reliable principles and methods, it contains inadequately supported conclusions, is not relevant to the issues at hand and would not be helpful to the trier of fact. "[W]hen an expert opinion is based on data, a methodology, or studies that are simply inadequate to support the conclusions reached, *Daubert* and Rule 702 mandate the exclusion of

that unreliable opinion testimony." *Amorgianos*, 303 F.3d at 266.

1. Rucinski's Alfabox Test 1 Conclusions That Infomir Has No Control Over STBs Lack A Reliable Methodology

In Section IV(a) of the Rucinski Rebuttal, Rucinski describes a "test" he conducted of an Infomir MAG254 "Alfabox" device, identified as the "Rucinski Alfabox." Rucinski Rebuttal at 10-20, §IV(a). Rucinski states that he conducted the test to "identify its configuration details reported by the software on the Rucinski Alfabox." *Id*. at 11. Rucinski describes how he plugged in the box to electrical power and a monitor and used the remote control to navigate around the screens of the device. *Id.* at 11-19. At the end of this section, Rucinski reports that he landed on a configuration settings screen showing an "Update URL" configuration value, which included the domain "firmware.iptvsys.com," which Rucinski refers to as the "Alfabox Firmware Domain." Id. at 19. Rucinski reports that he "found no evidence that the Alfabox Firmware Domain is supervised or controlled by Infomir." *Id*. at 4, 10, 20.

Based on the foregoing, Rucinski concludes "[g]iven that the Alfabox Firmware Domain contains the word 'firmware' it is likely that the Rucinski Alfabox is configured such that Infomir does not have the ability to supervise or control the firmware with which it is updated because the Rucinski Alfabox appears to update its firmware from the Alfabox Firmware Domain." In other words, even though Rucinski admits that he does not know who owns or controls the Alfabox Firmware Domain, he arbitrarily speculates that it must not be controlled by Infomir, a conclusion for which there is no evidentiary, scientific, or logical support. In doing so, Rucinski makes a significant speculative leap, without substantiating his conclusion, or citing to any authority. Additionally, he does not connect to Infomir's Stalker middleware, does not collect a PCAP and does not analyze whether the middleware permits Infomir to control the STB. This portion of the Rucinski expert testimony must therefore be excluded because it is completely without evidentiary

or logical foundation.

Mr. Rucinski also provides no evidence, authority, reliable methodology, or even mere argument as to how one can reasonably and reliably conclude that an internet domain (the Alfabox Firmware Domain) is not controlled by a specific entity (Infomir). He provides no explanation as to why the STB connects to this domain. He doesn't examine the firmware or software on the Rucinski Alfabox to see if that code directs the STB to connect to this domain. He doesn't investigate the ownership of the domain block or even to ask Infomir if it controlled the domain. The entire basis for his conclusion (i) he found no evidence that Infomir did control the domain, and (ii) the domain had the word "firmware" in it. An expert witness may be excluded if his or her proposed methodology is not sufficiently rigorous at each step. "[R]eliability within the meaning of Rule 702 requires a sufficiently rigorous analytical connection between that methodology and the expert's conclusions." *Nimely,* 414 F3d at 396. Because his methodology is baseless and flawed, Rucinski's proposed testimony regarding these conclusions should be excluded.

2. Rucinski's Bari Alfabox Text 1 Conclusions That Infomir Has No Control Over STBs Lack A Reliable Methodology

In Section IV(b) of the Rucinski Rebuttal, Rucinski describes another "test" he conducted of an Infomir MAG256 "Alfabox" device, this time the "Bari Alfabox." Rucinski Rebuttal at 20-25. This "test" was similar to the Rucinski Alfabox tests, and the "conclusions" were nearly identical. The difference was that the STBs ran different firmware, as described on Infomir's website. See https://soft.infomir.com/ (providing firmware update files for multiple STB models). Rucinski conducted no comparison of the Rucinski and Bari Alfaboxes. Again, without stating any reasons, presenting any evidence, or advancing any repeatable or reliable testing methodology such as connecting it with Infomir's middleware, collecting a PCAP and analyzing whether or not the middleware permitted Infomir to control the STB, Rucinski speculates that it is "likely that the

Bari Alfabox is configured such that Infomir does not have the ability to supervise or control the firmware with which it is updated…" Rucinski Rebuttal at 25.

Thus, the proposed testimony found at Section IV(b) of the Rucinski Rebuttal should be excluded for the same reasons that Rucinski's testimony in Section IV(a) should be excluded, namely, because it is utterly unreliable.

3. Rucinski's PCAP Analysis Conclusions Relating To Infomir's Lack of Involvement In Unlicensed Streaming Lack A Reliable Methodology

In Section VI of the Rucinski Rebuttal, Rucinski attempts to address whether Dmitri Dietrich's capture and analysis of network activity from Infomir MAG 256 Alfabox products shows whether "Infomir participates in sending unlicensed content." Rucinski Rebuttal at 32. During this analysis, Rucinski claims to have used the Wireshark program to perform "a case-insensitive search for 'Infomir'" in both the 'Info' field as well as the "contents" of each packet in Dietrich PCAP 2, and reports that no packets matched the "search" or "filter." Rucinski Rebuttal at 32. In essence: Rucinski reports that he eavesdropped on the conversations between the Infomir MAG 256 Alfabox and various computers on the internet, listening for the word "Infomir," and did not hear it.

Then, with no intervening analysis, logic, or explanation, Rucinski opines that "[i]f Infomir had participated in sending unlicensed content to the Dietrich Alfabox, it is likely that 'Infomir' would have appeared many times in either of these two searches." Rucinski Rebuttal at 33. This conclusory statement is utterly unsupported by any reliable scientific or analytical method or even a reasonable logical inference. It is akin to concluding, after eavesdropping on a conversation between individuals who may or may not be involved in organized crime (i.e. mobsters), that it is "likely" that if they had participated in any criminal activity with mob boss Tony Soprano, then Tony Soprano's name "would have appeared many times in" the transcripts of the wiretaps. Such

a conclusion fails to consider that persons involved in illegal activities, whether hapless mobsters or sophisticated television pirates, conceal such activities, including by speaking in codes or using aliases.

Rucinski's conclusion as to the likelihood of Infomir's participation in the distribution of unlicensed content is inadmissible because he does not present any rational, repeatable, or reliable explanation for why it should be so. For example, Rucinski did not try to support his conclusions by examining data streams relating to other IPTV STBs and content provider to show that such streams include the identities of the corporations facilitating the streaming. Likewise, Rucinski cited no convention, rule, internet standard, or other authority which would cause two devices communicating via the internet to include the identity of the corporations owning the devices in the communications. Rucinski could have investigated the IP addresses connecting to the STB but chose not to. In short, Rucinski has disclosed no authority, repeatable method, or logical inference from which he makes conclusions as to the likelihood of whether the word "Infomir" would appear in a pirate video data stream facilitated by Infomir LLC or its affiliates.

Inconsistently, the remainder of Section VI of the Rucinski Rebuttal shows that Rucinski draws the conclusion that video streams are not connected to Infomir even when the word "Infomir" does appear in URLs in a communication stream. This occurs when Rucinski reviews Dietrich PCAP 1 which he admits "contains several references to 'Infomir.'" Rucinski Rebuttal at 34-36. Nowhere does he explain why Infomir's name keeps appearing and he testified that he would need to do more research to determine whether the STBs are engaged in a handshake. Rucinski Tr. 159: 16-23. Nonetheless, his conclusion is unchanged – Rucinski "has [] not found any indication that either Dietrich PCAP 1 or Dietrich PCAP 2 demonstrate that Infomir participates in sending unlicensed content to STBs." *Id*. at 36. However, once again, Rucinski

provides no repeatable or reliable methodology, or even an explanation as to why his conclusion remains the same in each situation, an inconsistency that cannot be easily reconciled or explained away even if Rucinski did address it, which he does not, and thus demonstrates that his conclusions are mere speculation. "Expert testimony should be excluded if it is speculative or conjectural" *Boucher v. U.S. Suzuki Motor Corp.*, 73 F.3d at 21.

Because Infomir has failed to meet its burden of showing that Rucinski's opinions as to the likelihood of Infomir's participating in sending unlicensed content to STBs are unsupported by reliable and repeatable methodology, (as well as being internally inconsistent), Rucinski's proposed testimony in Section VI of the Rucinski Rebuttal should be excluded.

4. Rucinski's Analysis of The Effectiveness of Blacklisting Lacks A Reliable Methodology and is Self-Contradicting

Rucinski's analysis of Infomir's "blacklisting" capabilities with respect to the Infomir MAG STBs must be excluded because it is presented without any reliable methodology or supporting evidence, and because it is internally and logically inconsistent. This analysis is thus both inadmissible as well as unhelpful (and especially confusing) to a fact finder. First, Rucinski reports that, according to Infomir, "measures such as domain blacklisting were introduced to prevent its MAG 256 STBs and its MAG 254 STBs from accessing unlicensed video content." Rucinski Rebuttal at 37. Infomir alleges that it issued an update which prevented access to "23 websites." Rucinski Rebuttal at 37. These websites include known pirate TV operators such as Teleprom and NovoeTV. Rucinski Rebuttal at 37. Astonishingly, Rucinski "disagrees with Bari's opinions suggesting that blacklisting … is an effective or practical means to restrict or prevent broadcast of unlicensed IPTV content," But provides no industry literature to support this opinion. Rucinski Rebuttal at 37.

Following these conclusions, the Rucinski Rebuttal discusses how Rucinski tested various

Infomir's MAG STBs and discovered that "a MAG 256 STB with updated firmware can access portals associated with licensed video content but explicitly prohibits access to portals such as the Novoe TV Portal and the Teleprom Portal that are associated with allegedly unlicensed content." *Id.* at 75, *See generally*, Rucinski Rebuttal at 38 – 97. In other words, what Rucinski's report discloses is that, when Infomir bothers to do so, it can exercise sufficient control over STBs to restrict access to pirate TV content.

However, in Section IX of the Rucinski Rebuttal, Rucinski inexplicably, and without any repeatable or reliable methodology or support in industry literature, arrives at the opposite conclusion, opining that "[a]ttempting to counteract alleged infringement by updating firmware that blacklists domains is not an effective or practical solution for Infomir to restrict or prevent broadcast of unlicensed IPTV content in general." Rucinski Rebuttal at 99. In other words, after showing evidence that Infomir has effectively and practically restricted his own access to pirate TV providers such as Teleprom and NovoeTV, Rucinski concludes that doing so is impractical. Needless to say, this assertion is made without reference to any reliable or repeatable methodology.

Aside from Infomir, the Court may take judicial notice that other video device and STB providers restrict access to pirate content and provide "practical" and "effective" means to do so. Rucinski's primary arguments boil down to assertions that it would not be "practical" or "effective" to blacklist domains offering pirated content because it would require proactive monitoring, involve determinations about licenses, require subscriptions to third party IPTV services, or that users might hack the devices to disable firmware updates. Rucinski Rebuttal at 99-100. Putting aside the question of truthfulness, Rucinski provides no cost-benefit analysis that the Court or a fact-finder could double check, no estimates about costs, success rates, the likelihood of customer hacking, or the like that one could verify or falsify.

Moreover, the court may take judicial notice that Rucinski's analysis, like Rosenblatt's, is contradicted by Copyright Act's requirement of having an effective notice and takedown procedure that can be documented to a court. *See* 17 U.S.C. §512(c)(3)(a); *Viacom Int'l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 524 (S.D.N.Y. 2010), *judgment overturned on other grounds by Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012).

Thus, Rucinski's analysis with respect to "blacklisting" fails to present a reliable scientific methodology, and further because it is logically inconsistent and fails to account for obvious counterexamples susceptible to judicial notice, clearly failing to demonstrate in his report "the same level of intellectual rigor that characterizes the practice of an expert in the relevant field." *Kumho Tire Co. v. Carmichael*, 526 U.S. at 152. Therefore, the proposed testimony at Rucinski Rebuttal 37-97, and 99-102 should be excluded.

5. Rucinski's Summaries of Opinions Lack A Reliable Methodology

For the same reasons as discussed above, Rucinski's "Summary of Opinions," (Rucinski Rebuttal at 4-5) and any other summary or restatement of his opinions or conclusions with respect to inadmissible subject matter should also be excluded.

C. (ON BEHALF OF CHANNEL ONE) INFOMIR HAS NOT SATISFIED ITS DAUBERT BURDEN OF SHOWING ADMISSIBILITY BY A PREPONDERANCE OF THE EVIDENCE BECAUSE ROSENBLATT AND RUCINSKI CONSCIOUSLY AVOIDED DISCUSSING AND ANALYZING EVIDENCE OF ILLEGAL STREAMING COLLECTED BY CHANNEL ONE RUSSIA AND BROADCASTERS

Infomir's experts Rosenblatt and Rucinski should be excluded under the Daubert factors because they have purposefully avoided familiarity with the evidence of Infomir's knowledge of its customers' infringing uses supporting the infringement claims underlying this action. Furthermore, each expert has taken pains to engage in purported "testing" that is designed to

mislead the trier of fact and lead to false conclusions. *See* Fed. R. Evid. 403, 702. To determine whether Infomir is supporting alleged pirate NovoeTV, for example, an expert acting in good faith would purchase an access code, watch (infringing) programming, and analyze the IPTV stream with a network protocol analyzer such as Wireshark. In 2018, Plaintiffs provided a list of pirates to Infomir that included the website, login, password and the portal URL for eleven major pirates, including NovoeTV. (CHANNELONE002425). Infomir represented to the Court that it needed this information to investigate the alleged piracy. Plaintiffs resisted because this would cut off the ability to easily monitor piracy activities. The Court compelled production of the passwords and logins. (ECF 529). However, Rosenblatt and Rucinski each testified they did not configure an Infomir MAG 254 STB with these logins and passwords that would have permitted the type of reliable investigation that Infomir suggested to the Court would occur.

Channel One recently retained Lydia Vitkova to determine whether Infomir continued to support NovoeTV's infringing IPTV streaming services and Ms. Vitkova conducted just such a reliable test documented by a Wireshark .PCAP file. Dowd Decl., Ex. A (Declaration of Lydia Vitkova dated January 27, 2021). This test shows that Infomir STBs give a "handshake" to Infomir that permit the STBs to function. Well before Infomir's experts did their tests, Infomir was given an affidavit showing how to easily downgrade Infomir's firmware upgrade to avoid pirate blacklisting. Dowd Decl. Ex. B (dated September 11, 2017). Both Rosenblatt and Rucinski were aware of reliable procedures to be used to investigate whether or not Infomir is facilitating the unauthorized distribution of Broadcasters' content through NovoeTV by accessing it through Infomir MAG boxes and Infomir middleware to assess the effectiveness of Infomir's blacklisting measures. Because each chose not to use these reliable methods, their testimony should be excluded.

Similarly, Plaintiff Channel One commenced an action on March 19, 2018 captioned J*oint Stock Company "Channel One Russia Worldwide" v. Russian TV Company, et. al* 18 Civ. 2318 (LGS) and designated it as related to this action. During the course of that action, Channel One discovered invoices showing evidence of Infomir providing 3,000 customized MAG 256 STBs to infringer Russian TV Company. Dowd Decl. Ex. C (dated February 2, 2017). As it was discovered, this evidence was timely provided to Infomir pursuant to Rule 26 of the Federal Rules of Civil Procedure for use in this action.

Rather than testing one of Infomir's devices, providing evidence of the testing to the court, and explaining the mechanics of IPTV streaming in a straightforward manner, each of Infomir's experts engaged in evasion and obfuscation. *Chill v Calamos Advisors LLC*, 417 F. Supp. 3d 208, 229 (SDNY 2019). Grounds for finding a witness incredible include, inter alia, evasive, inconsistent, contradictory or implausible testimony. *See, e.g., Latin Am. Music Co., Inc Spanish Broad. Sys., Inc.*, 254 F. 3d 584, 589–90 (S.D.N.Y. 2017). If the Court finds that any portion of a witness's testimony was intentionally untruthful or misleading, the Court can elect, under the doctrine of *falsus in uno falsus in omnibus*, to reject the entirety of the witness's testimony. *Hernandez v. NJK Contractors, Inc.*, No. 09 Civ. 4812 (RER), 2015 WL 1966355, at *31 (E.D.N.Y. May 1, 2015) (citations omitted).

Because Rosenblatt and Rucinski have been evasive to the point of willful blindness, their testimony should be excluded. The Rosenblatt Report and Rucinski Rebuttal are not based on reliable methodology, nor sufficient facts or data, as detailed above. Neither expert analyzed an operational Infomir IPTV platform: MAG STB, Stalker middleware, nor a MAGic solution project. *See* SAC ¶¶ 138-47 (describing Infomir's platform). Rosenblatt failed to examine a configured Infomir STB in his report. (Rosenblatt Tr. 34:20- 36:22; 216:16-217:16). Rucinski

analyzed STBs provided by Infomir but failed to examine the firmware running on the MAG STBs and Alfabox to determine how the firmware directed connections to Stalker Middleware, requested firmware updates that purportedly enable domain blocking (Rucinski Tr. 125:12-126:11). Rucinski also did not know if Infomir initiated any blacklisting via firmware prior to June 13, 2017. (Rucinski Tr.169:2-9). He also failed to test domain blocking on the Alfabox, an STB provided by an unlicensed provider.

Although Mr. Goldfedib described the role of middleware, which does not run on an STB, as "the software which communicate with different applications in the service provider's environment." (Goldfedib Tr. 133: 22-134:9); *see also* June 28, 2017 Goldfedib Decl. (ECF 300) ¶ 50 ("Middleware is a necessary technical component of an IPTV provide system."). Despite this, Rosenblatt failed to examine configured Stalker Middleware and Rucinski did not examine Stalker Middleware at all. (Rosenblatt ¶ 34; Rucinski Tr. 104:6-13; 113:5-11; 233:16- 24; 234:25-235:4).

The MAGic solution is a key component of enabling Infomir STBs to encourage piracy. (Am Cplt. ¶¶ 138-47). Goldfedib has also affirmed that the MAGic solution enables "customers to configure, integrate, and customize Infomir set-top boxes and middleware for use with [an IPTV provider's] project. Godlfedib Decl. ¶ 46. Rucinski and Rosenblatt also testified that they never examined an operational MAGic solution. (Rucinski Tr. 246:22-247:6; Rosenblatt Tr. 10:4-13). Despite opining about the use of Infomir STBs by licensed and unlicensed providers, neither Infomir expert has reviewed a customer list or an Infomir sales invoice. (Rucinski 97:6-99:13; Rosenblatt 114:11-16, 252:22-253:4). Rosenblatt cannot reasonably conclude that an Infomir STB has substantial non-infringing uses when he examined an unconfigured STB, unconfigured Stalker Middleware and failed to examine a functioning IPTV system that uses Infomir's platform.

By contrast, the Vitkova declaration describing her investigation of the MAG 250 STB connected to NovoeTV shows the type of analysis that Rosenblatt and Rucinski could have done but failed to do. Vitkova was able to show that NovoeTV was not blocked with the latest Firmware on the MAG 250 (Vitkova ¶¶ 37-39). Vitkova found that the STB made a "handshake" to a server controlled by Infomir while connected to the NovoeTV service. (Vitkova ¶¶ 44, 49). Vitkova's findings undermine the methods used by Rucinski, who admitted a deeper investigation may have revealed a handshake took place. (Rucinski Tr. 159:16-23). Rucinski obscured (or concealed) the results of any testing he may have done because he did not create a PCAP in his rebuttal report while examining Infomir STBs. Examining an STB in isolation fails to provide a complete analysis of whether the Stalker Middleware is used to distribute unauthorized satellite communications or with knowledge that it will be used primarily as a device to assist in the distribution of unauthorized satellite communications.

Infomir's production of shipping invoice shows it imported over 550,000 STBs through 2017. (ECF 548-9 to 548-19). Those shipping invoices do not show the importation of the MAG 420w1 nor the MAG 425A. Infomir has not supplemented its production to show that these STBs were ever imported into the United States. Nevertheless, Rosenblatt opines that DRM capabilities of the MAG 425A, approved by Google, are representative of the DRM capabilities of Linux MAG STBs, like the MAG 254 and MAG 256. (Rosenblatt Report ¶ 59)(citing DRM capabilities of the MAG 425A). Infomir has not produced documents evidencing sales to any legitimate (non-pirate) customers in the Americas, including the model of STB sold to (1) Rodeo Internet (Rosenblatt Report ¶¶ 25, 75); (2) Naicom (*Id.* ¶¶ 25, 75); (3) Karostream (*Id.*¶ 26); (4) BH Bostel Net (*Id.*¶ 26); (5) Megogo (*Id.*¶ 26); (6) Kartina (*Id.*¶ 26); (7) Teko IPTV (*Id.*¶ 76); or (8) NetSolid (*Id.*¶ 77). The only Infomir sales invoices obtained in discovery were those of Russian TV Company,

Inc. and its affiliates (ECF 736-23)(showing approximately 35,000 STBs sold to an IPTV provider not licensed by Channel One). Mr. Rosenblattt cannot reliably conclude Infomir STBs have substantial non-infringing uses without any knowledge of how many STBs Infomir's eight disclosed "legitimate" customers bought or how those STBs were configured. (*Id.* ¶¶ 73-79). Because evidence supporting any non-infringing use was not supplied in discovery and because Channel One thus has no opportunity to cross examine Mr. Goldfedib or Anneta Rozenberg about these customers, Infomir should not be permitted to use experts to engage in an end-run around the non-dislosure, particularly where, as here, the non-disclosure has rendered the experts' conclusions unreliable.

Infomir's failure to produce evidence that supposedly supports the experts' conclusions prevented meaningful cross-examination or analysis. For example, Infomir has not produced any executable firmware images that operates its Linux STBs that Rucinski claims to have analyzed. Infomir's purported anti-piracy program relies on firmware updates that purportedly block infringing domains and URLs from being used on an Infomir device. (Rucinski at 37-97). Rucinski discloses only that he considered "firmware images corresponding to Infomir STBs." Rucinski Rebuttal ¶ 18 at 3. Rucinski then testified that he "looked at" at "some executable versions of [Infomir] firmware." (Rucinski Tr. at 256). His testimony does not clarify what firmware versions he examined, and such firmware was never produced in discovery so it is impossible for Broadcasters to test his conclusions about the efficacy of firmware in blocking piracy URLs, or even verify that he even looked at the firmware

Rule 703 of the Federal Rules of Evidence requires that expert reports are based either on hearsay evidence qualified by the expert based on industry standards, or otherwise on admissible, authenticated evidence. Infomir withheld (1) documentary evidence of purported non-infringing

use of their STBs (Rosenblatt ¶¶ 25-26, 75-77) and (2) "Firmware images corresponding to Infomir STBs" listed in the materials considered by Rucinski (Rucinski at 3). Because Mr. Rucinski relies on inadmissible hearsay materials in reaching his conclusions regarding Infomir firmware, his conclusions should be excluded. Fed. R. Evid.703. Because Mr. Rosenblatt relies on inadmissible hearsay materials in reaching his conclusions regarding non-infringing uses of Infomir STBs and software, his conclusions should be excluded. Fed. R. Evid.703. Therefore, Infomir cannot reliably support its twelfth (substantial non-infringing use) and thirteenth (lack of volition) affirmative defenses because it has not met its burden of producing admissible evidence that can be tested.

Neither expert had sufficient data from which to draw any conclusions regarding Infomir's purported anti-piracy efforts. For example, Courts evaluating antipiracy efforts count the number of takedowns and complaints, together with response times in weighing the effectiveness of anti-piracy programs. Rucinski testimony that Infomir's blacklisting is an antipiracy system is offered in Infomir's Thirteenth Affirmative Defense that the alleged infringement was not caused by a volitional act of Infomir. (ECF 251). However, Mr. Rucinski's testimony relating to whether Infomir's purported blacklisting constitutes an antipiracy system is doubtful because there is no evidence showing the scale on which the blacklisting was implemented or data on its effectiveness. (*Compare* Rucinski Tr. 181:5-182:2).

V. CONCLUSION

For the reasons stated above, Infomir's proposed expert testimony does not meet the requirements for admissibility under Fed. R. Evid 702 or 703 and should be excluded because Rosenblatt's and Rucinski's opinions are both irrelevant and unreliable; they contain large analytical gaps, lack sufficient data, they both misstate the issues relevant to the case and merely state speculative opinions unsupported by any reliable, repeatable methodology. In addition,

Channel One argues that Infomir has not satisfied its *Daubert* burden of showing admissibility by a preponderance of the evidence because Rosenblatt and Rucinski consciously avoided discussing and analyzing evidence of illegal streaming collected by Channel One Russia and Broadcasters. The two proffered reports are so rife with misleading and evasive information that the testimony should be excluded in full.

In the alternative, if this Court sees fit to include any of the testimony, it should be pared to exclude those parts specifically referenced above which do not meet the *Daubert* standard of admissibility.

February 19, 2021

Respectfully Submitted,

/s/ Eugene D. Kublanovsky

KUBLANOVSKY LAW LLC
Eugene D. Kublanovsky
Allison Charles
Erik Dykema
10 East 39th Street, 12th Floor
New York, New York 10016
Tel: 212.729.4707
Email: eugene@edklaw.com
Email: allison@edklaw.com
Email: erik@edklaw.com

Attorneys for Plaintiffs Closed Joint Stock Company CTC Network, Closed Joint Stock Company TV Darial, Closed Joint Stock Company New Channel, Limited Liability Company Rain TV-Channel, Limited Liability Company Global Entertainment TV

/s/ Raymond J. Dowd

DUNNINGTON BARTHOLOW & MILLER LLP
Raymond J. Dowd
Hardin Rowley
230 Park Avenue 21st Floor
New York NY 10169
Tel: (212) 682-8811

Email: rdowd @dunnington.com
Email: hrowley@dunnington.com

Attorneys for Joint Stock Company "Channel One Russia Worldwide"